PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 03 February 1999 (03.02.99)	
International application No. PCT/US98/11634	**Applicant's or agent's file reference** RCA 88674
International filing date (day/month/year) 05 June 1998 (05.06.98)	**Priority date** (day/month/year) 06 June 1997 (06.06.97)
Applicant ESKICIOGLU, Ahmet, Mursit	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

21 December 1998 (21.12.98)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer S. Baharlou
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
RCA 88674		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US 98/ 11634	05/06/1998	06/06/1997

Applicant

THOMSON CONSUMER ELECTRONICS, INC. et al.

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. [ ] **Certain claims were found unsearchable** (see Box I).

2. [ ] **Unity of invention is lacking** (see Box II).

3. [ ] The international application contains disclosure of a **nucleotide and/or amino acid sequence listing** and the international search was carried out on the basis of the sequence listing
   - [ ] filed with the international application.
   - [ ] furnished by the applicant separately from the international application,
     - [ ] but not accompanied by a statement to the effect that it did not include matter going beyond the disclosure in the international application as filed.
   - [ ] Transcribed by this Authority

4. With regard to the **title,**
   - [X] the text is approved as submitted by the applicant
   - [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   - [X] the text is approved as submitted by the applicant
   - [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this International Search Report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is:
   Figure No. 3
   - [X] as suggested by the applicant.
   - [ ] because the applicant failed to suggest a figure.
   - [ ] because this figure better characterizes the invention.
   - [ ] None of the figures.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04N 7/167, 7/16, 5/00

A1

(11) International Publication Number: **WO 98/56180**

(43) International Publication Date: 10 December 1998 (10.12.98)

(21) International Application Number: PCT/US98/11634

(22) International Filing Date: 5 June 1998 (05.06.98)

(30) Priority Data:
60/048,852 6 June 1997 (06.06.97) US

(71) Applicant *(for all designated States except US)*: THOMSON CONSUMER ELECTRONICS, INC. [US/US]; 10330 North Meridian Street, Indianapolis, IN 46290–1024 (US).

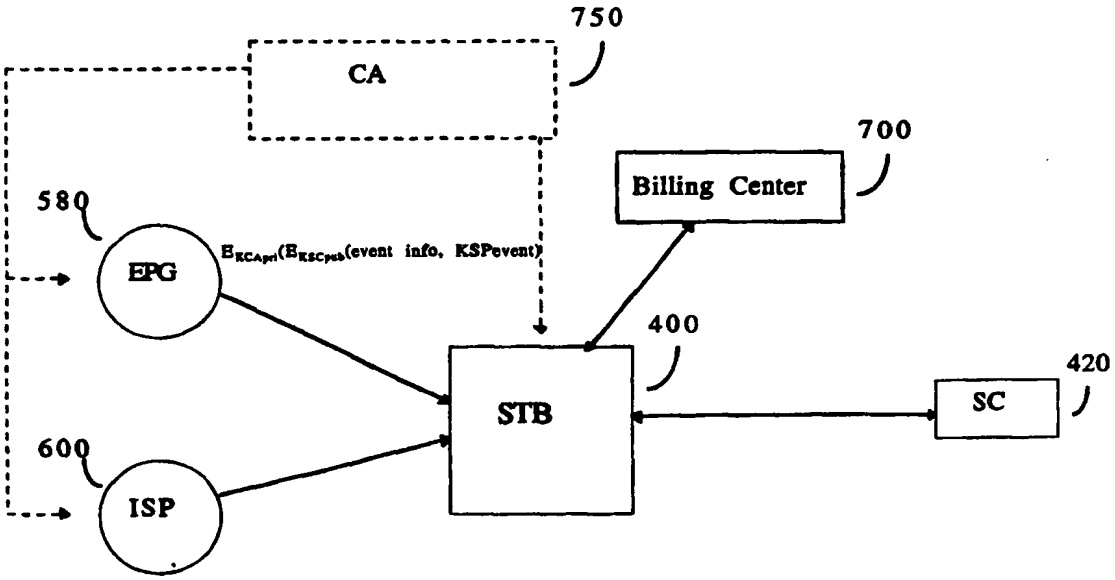
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: ESKICIOGLU, Ahmet, Mursit [TR/US]; 8235 Lakeshore Trail No. 125, Indianapolis, IN 46250 (US).

(74) Agents: TRIPOLI, Joseph, S. et al.; GE & RCA Licensing Management Operation, Inc., P.O. Box 5312, Princeton, NJ 08543 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: GLOBAL CONDITIONAL ACCESS SYSTEM FOR BROADCAST SERVICES



(57) Abstract

A method for managing access to a scrambled event, selected from an electronic program guide, of a service provider (including broadcast television networks, cable television networks, digital satellite systems, and internet service providers). Access to the event is only achieved if the descrambling key is obtained from a digitally signed message associated with the event in the electronic program guide. Authentication of the electronic program guide provider involves decrypting the digital signature using a public key of the guide provider.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

GLOBAL CONDITIONAL ACCESS SYSTEM FOR BROADCAST SERVICES

Field of the Invention

This invention concerns a system for providing conditional access (i.e., managing access) to a consumer electronic device, such as a set-top box or a digital television, that is capable of receiving broadcast digital streams from a variety of sources, such as, broadcast television networks, cable television networks, digital satellite systems, internet service providers and sources of electronic list of events.

Background of the Invention

Today, as depicted in Figure 1, a user may receive services from a variety of service providers, such as broadcast television networks 22, cable television networks 24, digital satellite systems 26, and internet service providers 28. System 10 of Figure 1 defines the present configuration for receiving services from such service providers. Most television receivers 12 are capable of receiving unscrambled, information or programs directly from broadcast and cable networks. Cable networks providing scrambled or encrypted programs usually require a separate stand-alone device 16a, 16b (e.g., a set-top box) to descramble or decrypt the program. Similarly, digital satellite systems usually provide scrambled or encrypted programs that also require the use of a separate set-top box. These set-top boxes may utilize a removable smart card 18a, 18b which contain the necessary decrypting algorithms and keys. Typically, a separate set-top box is required for each service

provider. Connections to the internet or world-wide web (web) are usually handled via a personal computer 14, or the like, and a modem 20. Traditionally, access to the internet is managed using a specially designed software package loaded onto the computer; this software enables a user to connect to an internet service provider who acts as the gate keeper to the web. The user typically pays a monthly fee to the service provider for access to the internet, either on a limited or unlimited basis. As one would expect there are numerous service providers, each which requires specialized software for access.

Summary of the Invention

The manufacturers of these digital televisions and set-top boxes may desire that they be compensated by the service provider for each connection to the service emanating from the box. Thus, the flexibility of open hardware architecture of the televisions and the set-top boxes in combination with a competitive market for such devices necessitates the need to provide a system for managing access so that the manufacturer is compensated for any use of its hardware to access any selected service provider. This invention resides, in part, in recognition of the described problem and, in part, in providing a solution to the problem.

An event or program as described herein comprises one of the following: (1) audio/visual data such as a movie, weekly "television" show or a documentary; (2) textual data such as an electronic magazine, paper, or weather news; (3) computer software; (4) binary data such as images or (5) HTML data (e.g., web pages). These service providers include any provider broadcasting events, for example,

traditional broadcast television networks, cable networks, digital satellite networks, providers of electronic list of events, such as electronic program guide providers, and in certain cases internet service providers.

Generally, the present invention defines a method for providing conditional access to a broadcast event from a service provider. That is, this method comprises receiving an electronic list of events, such as an electronic program guide, from a list provider, wherein the list has a digitally signed message corresponding to each event of the list or guide, the digitally signed message comprises a message encrypted using a second public key and a digital signature created using a first private key. The method further comprises selecting an event from the list; receiving the digitally signed message corresponding to the selected event; authenticating the list provider; decrypting the message using a second private key to obtain an event key; receiving the selected event which is scrambled using the event key; and descrambling the selected event using the event key to provide a descrambled event.

In accordance with one aspect of the present invention, the steps of decrypting the message, receiving the selected event, and descrambling the selected event are performed in a removable smart card coupled to the device wherein the second private key is stored in the smart card.

In accordance with another aspect of the present invention, the message comprises event information which can be decrypted using the second private key. The event information further being

stored in the smart card having a card body with a plurality of terminals arranged on a surface of the card body in accordance with one of ISO standard 7816 or PCMCIA card standards.

In accordance with yet another aspect of the present invention, a system for managing conditional access between a service provider and a device having a smart card coupled thereto, the device performing the steps of: receiving an electronic program guide having a digitally signed message corresponding to each event in the guide wherein each digitally signed message comprises a message encrypted using a smart card public key and a digital signature created using a guide provider private key; selecting an event from the guide; receiving the digitally signed message corresponding to the selected event; authenticating the guide provider by decrypting the digital signature; passing the message to a smart card; decrypting the message to obtain event information and a symmetric key; storing the event information in the smart card and updating account information; receiving the selected event which is scrambled using the symmetric key; and descrambling the selected event using the symmetric key to generate a descrambled event.

In accordance with yet another aspect of the present invention, a system for managing access between a service provider and a device having a smart card coupled thereto, the device performing the steps of: receiving an electronic program guide having a digital certificate and a separate message corresponding to each event in the guide, each of the digital certificates being encrypted using a first guide private key, the separate messages being encrypted using a smart card public key and containing an associated signature created

using a second guide private key; selecting an event from the guide; receiving the digital certificate, message and associated digital signature corresponding to the selected event; authenticating the guide provider; passing the message to a smart card; decrypting the message using a smart card private key to obtain event information and a symmetric key; storing the event information in the smart card and updating account information based on the event information; receiving the selected event wherein the selected event is scrambled using the symmetric key; and descrambling the selected event using the symmetric key to generate a descrambled event.

These and other aspects of the invention will be explained with reference to a preferred embodiment of the invention shown in the accompanying Drawings.

Brief Description of the Drawing

Figure 1 is a block diagram illustrating a prior art configuration for interconnecting consumer electronic devices to a variety of service providers.

Figure 2 is a block diagram illustrating one architecture for interfacing a common set-top box to a variety of service providers.

Figure 3 is a block diagram of an exemplary implementation of a system for managing access to a device in accordance with the invention; and

Figure 4 is a block diagram of another exemplary implementation of the system of Figure 3.

Detailed Description of the Drawing

The present invention provides a conditional access system which may be utilized to obtain services from one of a plurality of sources. The conditional access system when implemented within a set-top box permits the set-top box to authenticate the service provider before a broadcast event is purchased and uses a smart card for decrypting the encrypted event received from the service provider. Alternately, the functionality of the smart card may be embedded within the set-top box. Such a conditional access system may act as a toll bridge for access to services thereby permitting a mechanism for the manufacturer of the set-top box to collect fees based on use of its set-top box. Similarly, this invention may be implemented within a digital television; for simplicity, the below description of the invention will be directed towards an implementation using a set-top box and a smart card.

In Figure 2, system 30 depicts the general architecture for managing access to a set-top box (STB) 40. Smart Card (SC) 42 is inserted into or coupled to a smart card reader (not shown) of STB 40; an internal bus 45 interconnects STB 40 and SC 42 thereby permitting the transfer of data therebetween. Such smart cards include ISO 7816 cards complying with National Renewable Security Standard (NRSS) Part A or PCMCIA cards complying with NRSS Part B. Conceptually, when such a smart card is coupled to a smart card reader, the functionality of the smart card may be considered to be a

part of the functionality of the set-top box thus removing the "boundaries" created by the physical card body of the smart card.

STB 40 can receive services from a plurality of service providers (SPs), such as a broadcast television SP 50, a cable television SP 52, a satellite system SP 54, an internet SP 56, and an electronic event guide SP 58. Certificate authority (CA) 75 is not directly connected to either the service providers or STB 40 but issues digital certificates and public and private key pairs which are used as explained below. A set-top box public key is provided to the manufacturers of the devices and is stored therein before the product is shipped to the consumer. It is within the scope of this invention that the role of certificate authority 75 may be performed by the service providers in collaboration with the manufacturer of the STB 40. Billing system 70 is utilized to manage the user's accounts; updated information is provided as user's make arrangements to purchase additional services and as these services are consumed or used.

The general architecture of system 30 lends itself to achieving the goal of providing a vehicle for the manufacturer of the set-top box to collect a fee based on the consumer's use of the box to access an event. One adaptation of the general architecture would be to utilize a common conditional access and billing system encompassing all manufacturers and service providers. A problem with such an adaptation is that it may be difficult to obtain consensus amongst the various service providers and manufacturers of the set-top boxes. Another problem is that all the events would be encrypted using the public key of STB 40 and decrypted in SC 42 utilizing a

stored private key of STB 40; thus if the private key were to be compromised the security of the entire system would collapse.

The conditional access system of the present invention, which overcomes the above problems, will be described in relation to system 300 as shown in Figure 3. This conditional access system is based on authentication of the service provider communicating with STB 400 prior to purchasing a broadcast event from the service provider. In one embodiment of this conditional access system a combination of both an asymmetric key system (i.e., public-key system) and a symmetric key system is used. However, this invention is not limited to such an embodiment requiring symmetric keys as described below.

Symmetric key cryptography involves the use of the same algorithm and key for both encryption and decryption. The foundation of public-key cryptography is the use of two related keys, one public and one private. The private key is a secret key and it is computationally unfeasible to deduce the private key from the public key which is publicly available. Anyone with a public key can encrypt a message but only the person or device having the associated and predetermined private key can decrypt it. Similarly, a message can be encrypted by a private key and anyone with access to the public key can decrypt that message. Encrypting messages using a private key may be referred to as "signing" because anyone holding the public key can verify that the message was sent by the party having the private key. This may be thought of as being analogous to verifying a signature on a document.

A digitally signed message is a message sent in the clear (i.e., unencrypted) having a signature attached thereto. The attached signature is produced by encrypting either the message itself or a digest of the message; a digest of the message is obtained by hashing the message. (Hashing involves subjecting the message to a one-way hashing algorithm, such as MD5 developed by Ron Rivest or SHA-1 developed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) prior to encrypting the message.) Thus the recipient of the signed message can verify the source or origin of the message. (In comparison, a public key certificate or digital certificate is a message, containing a public key of the sending device, sent in the clear having a signature attached thereto.) Unilateral authentication of a service provider connected to the set-top box is achieved by passing such digitally signed messages between the service provider and the set-top box and verifying the signature. Signature verification involves checking the signature by decryption. Particularly, these messages contain at least information associated with the service provider passing the message or the selected event from the service provider and may contain the service provider's public key. These digitally signed messages, which may have signatures created by independent certificate authority 75, are stored by the service provider.

The following nomenclature will be utilized in the below description of the present conditional access system.

KSCpub	SC's public key
KSCpri	SC's private key

KCApub CA's Public Key used to verify signatures

KCApri CA's Private Key used to create signatures

KSPevent A service provider's event key

Conditional access system 300 of Figure 3 includes STB 400 having SC 420 coupled to a card reader (not shown); STB 400 communicates with billing center 700, a plurality of service providers (for simplicity, only one service provider, SP 600, is shown) and EPG 580. As discussed above, the functionality of SC 420 could be integrated into STB 400 and STB 400 could be a digital television. EPG 580 may be a separate service provider wherein electronic program guides containing listings of events from a plurality of service providers may be accessed. Alternately, EPG 580 may represent only a listing of events from a single service provider.

EPG 580 has a unique digitally signed and encrypted message associated with each event. This message is encrypted by KSCpub and is signed using KCApri, the private key that CA 750 assigned to EPG 580. The encrypted message may include information corresponding to the selected event and an event key, KSPevent.

After STB 400 is activated, SC 420 is coupled to a card reader of STB 400 (not shown), and in response to a user selecting a desired event from EPG 580, EPG 580 downloads the corresponding digitally signed message into STB 400. EPG 580 must be authenticated to ensure that the digitally signed message was received from the desired provider. This authentication involves

decrypting the digital signature in STB 400 using KCApub. KCApub is the public key that CA 750 assigned to EPG 580 and is stored in STB 400. If EPG 580 is not authenticated, STB 400 provides an error indication to the user. Authentication of EPG 580 requires that a pre-existing agreement exists between the electronic guide provider source and the manufacturer of STB 400. This is because without such an agreement CA 750 would not provide KCApri to the source of electronic program guide.

After STB 400 authenticates EPG 580, the encrypted message is passed to SC 420 for decryption. SC 420 decrypts the message using KSCpri, which is stored therein, to obtain the data corresponding to the selected event and the event key. This data may include data relating to channel identity, date and time stamp, event identity, and payment amount. This data is stored in a memory device within SC 420 and is used to update the user account information. The updated account information can be passed to billing center 700 using signed messages.

The event key is retained within SC 420 thereby reducing the possibility of observing the key. The event key is used to descramble, in SC 420, the selected event received from the service provider; SC 420 provides a descrambled program to STB 400. Alternately, the event key could be passed back to STB 400 and used to descramble or decrypt the selected event in STB 400.

If the functionality of the smart card is embedded in the set-top box, the encrypted message would be decrypted within STB 400 and the event information would be stored within the set-top

box. Similarly, the event key would remain in the set-top box and be used to descramble the selected event within STB 400.

System 300', as depicted in Figure 4, shows an alternative exemplary embodiment of the present invention wherein a certification hierarchy may be employed to avoid the certificate authority "signing" every message sent by a service provider. Certificate authority 750' generates a digital certificate for the public key of the service provider. The service provider, then in turn, would generate digitally signed messages using the corresponding private key of the service provider. That is, in response to a user selecting a desired event from EPG 580', EPG 580' downloads a digital certificate and a digitally signed message into STB 400'. The digital certificate is encrypted using KCApri and contains the service provider's public key, KSPpub. The digitally signed message is encrypted by the public key of SC 420', KSCpub, and is signed using the service provider's private key, KSPpri. The encrypted message may include information or data corresponding to the selected event and an event key, KSPevent.

In the same manner as for EPG 580 in the embodiment in Figure 3, EPG 580' must be authenticated. This authentication involves decrypting the digital certificate in STB 400' using KCApub, which is stored therein to obtain KSPpub, and decrypting the digitally signed message in STB 400' using KSPpub.

In another embodiment of the present invention, each unique digitally signed message corresponding to an event listed in the electronic program guide would have an associated encrypted

message. This encrypted message would only contain information related to the event, that is, the event key would not be included. In such an embodiment, public key cryptography may be used to encrypt the broadcast event. The electronic program guide must still be authenticated in STB 400 as described above. However, the decrypted message only contains information corresponding to the selected event. This information is stored and must be used by SC 420 to determine the private key for decrypting the event. In this embodiment utilizing public key cryptography, key transport is not needed.

The present invention has been described in terms of exemplary embodiments in which a single smart card cooperates with a single set-top box to manage access to a single service provider. However, it is within the scope of this invention to provide a conditional access system which may be extended to permit the smart card to "roam" across (i.e., provide conditional access between) multiple service providers and multiple manufacturers of the set-top boxes.

The robustness of the defined system may be increased by encrypting portions of the event with different keys included in the broadcast stream. These keys may be protected using the symmetric key received from the electronic program source.

While the invention has been described in detail with respect to numerous embodiments thereof, it will be apparent that upon reading and understanding of the foregoing, numerous alterations to the described embodiment will occur to those skilled in

the art and it is intended to include such alterations within the scope of the appended claims.

Claims

1. A method for managing access to an event of a service provider, said method comprising:

(a) receiving in a device an electronic list of events from a list provider, said list having a digitally signed message corresponding to each event in said list, each of said digitally signed messages comprise a message encrypted using a second public key and a digital signature created using a first private key;

(b) selecting an event from said list;

(c) receiving in said device said digitally signed message corresponding to the selected event;

(d) authenticating said list provider, using a first public key, in response to said digital signature;

(e) decrypting said message using a second private key to obtain an event key;

(f) receiving from the service provider said selected event, said selected event being scrambled using said event key; and

(g) descrambling said selected event using said event key to provide a descrambled event.

2. The method of Claim 1 wherein the steps of decrypting said message, receiving said selected event, and descrambling said selected event are performed in a smart card coupled to the device, said second private and public keys being associated with said smart card and said second private key being stored in said smart card.

3. The method of Claim 2 wherein said message further comprises event information, said event information being decrypted using said second private key.

4. The method of Claim 3 further comprising the step of storing said event information, wherein said step of storing said event information is performed in said removable smart card.

5. The method of Claim 4 wherein said smart card has a card body having a plurality of terminals arranged on a surface of said card body in accordance with one of ISO 7816 and PCMCIA card standards.

6. The method of Claim 5 wherein the step of authenticating comprises decrypting said digital signature in said device to verify the origin of said message.

7. The method of Claim 6 wherein said first public key is stored in said device.

8. The method of Claim 4 wherein said event information comprises channel identification data, event identity data, date and time stamp data, and billing data.

9. The method of Claim 3 further comprising the step of storing said event information, wherein said step of storing said event information is performed in said device.

10. The method of Claim 1 wherein said digital signature, said first public key and said first private key are issued by an independent certificate authority and are associated with said list provider.

11. The method of Claim 10 wherein said device is a digital television.

12. The method of Claim 10 wherein said device is a set-top box.

13. The method of Claim 4 wherein said event information is used within said device to update said user's account information.

14. The method of Claim 13 wherein said event information is downloaded to an independent billing center to update a user's account information.

15. In combination in a system for managing access between a service provider and a device having a smart card coupled thereto, said device performing the steps of:

(a) receiving an electronic program guide from a guide provider, said guide having a digitally signed message corresponding to each event in said guide, each of said digitally signed messages comprise a message encrypted using a public key of the smart card and a digital signature created using a private key of said guide provider;

(b) selecting an event from said guide;

(c) receiving said digitally signed message corresponding to the selected event;

(d) authenticating said guide provider by decrypting said digital signature using a public key of said guide provider, said guide public key being stored in said device;

(e) passing said message to a smart card coupled to the device;

(f) decrypting said message using a private key of the smart card to obtain event information and a symmetric key, said smart card private key being stored within the smart card;

(g) storing said event information in the smart card and updating account information based on said event information;

(h) receiving from the service provider said selected event, said selected event being scrambled using said symmetric key; and

(i) descrambling, in said smart card, said selected event using said symmetric key to generate a descrambled event.

16. The combination of Claim 15 wherein the device is a set-top box.

17. The combination of Claim 15 wherein the device is a digital television.

18. In combination in a system for managing access between a service provider and a device having a smart card coupled thereto, said device performing the steps of:

(a) receiving an electronic program guide, said guide having a digital certificate and a separate message corresponding to each event in said guide, each of said digital certificates being encrypted using a first private key of said guide, said separate message being encrypted using a public key of the smart card and having an associated digital signature created using a second private key of said guide;

(b) selecting an event from said guide;

(c) receiving said digital certificate, said message and said digital signature corresponding to the selected event;

(d) authenticating said guide provider by decrypting said digital certificate using a first public key of said guide to obtain a second public key of said guide, and decrypting said digital signature using said second guide public key, said first guide public key being stored in the device;

(e) passing said message to said smart card;

(f) decrypting said message using a s private key of the smart card to obtain event information and a symmetric key, said smart card private key being stored within the smart card;

(g) storing said event information in the smart card and updating account information based on said event information;

(h) receiving from the service provider said selected event, said selected event being scrambled using said symmetric key; and

(i) descrambling, in said smart card, said selected event using said symmetric key to generate a descrambled event.

19. The combination of Claim 18 wherein the device is a set-top box.

20. The combination of Claim 18 wherein the device is a digital television.

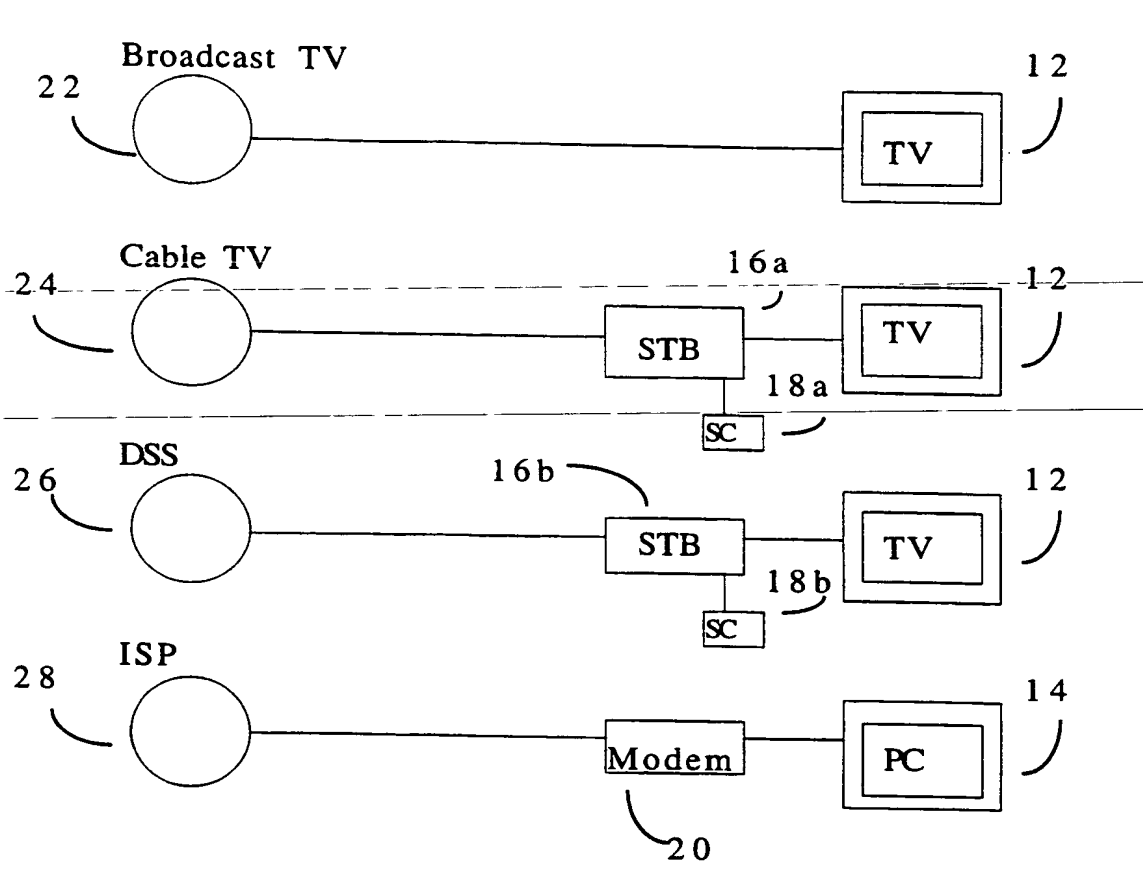

10
Broadcast TV
22
12
TV
Cable TV
24
16a
12
STB
TV
18a
SC
DSS
26
16b
12
STB
TV
18b
SC
ISP
28
14
Modem
PC
20
PRIOR ART

Fig 1

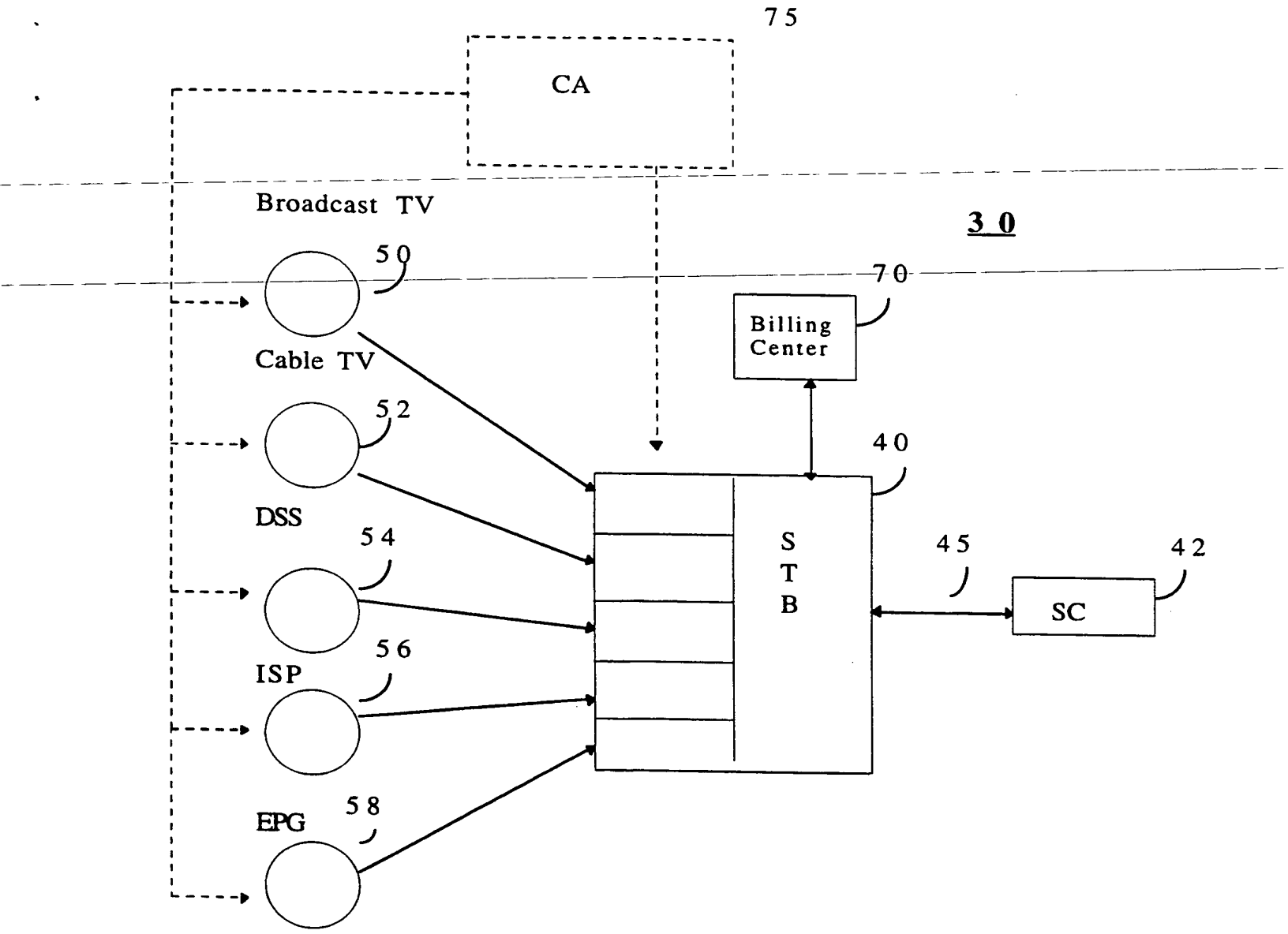

75
CA
Broadcast TV
30
50
70
Billing Center
Cable TV
52
40
DSS
54
S
T
B
45
42
SC
56
ISP
58
EPG

Fig 2.

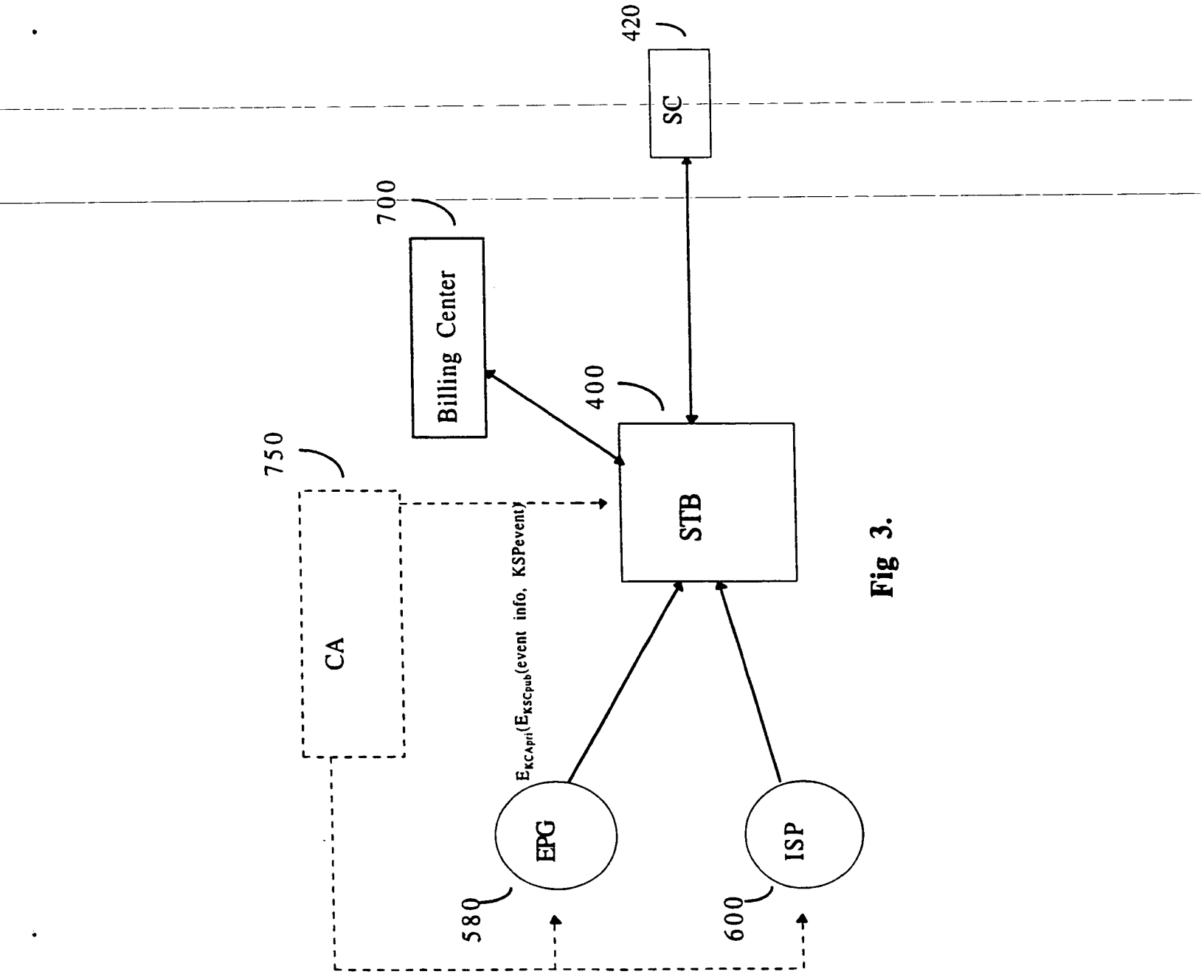

420
SC
700
Billing Center
400
750
STB
CA
$E_{KCApril}(E_{KSCpub}$(event info, KSPevent))
EPG
ISP
580
600

Fig 3.

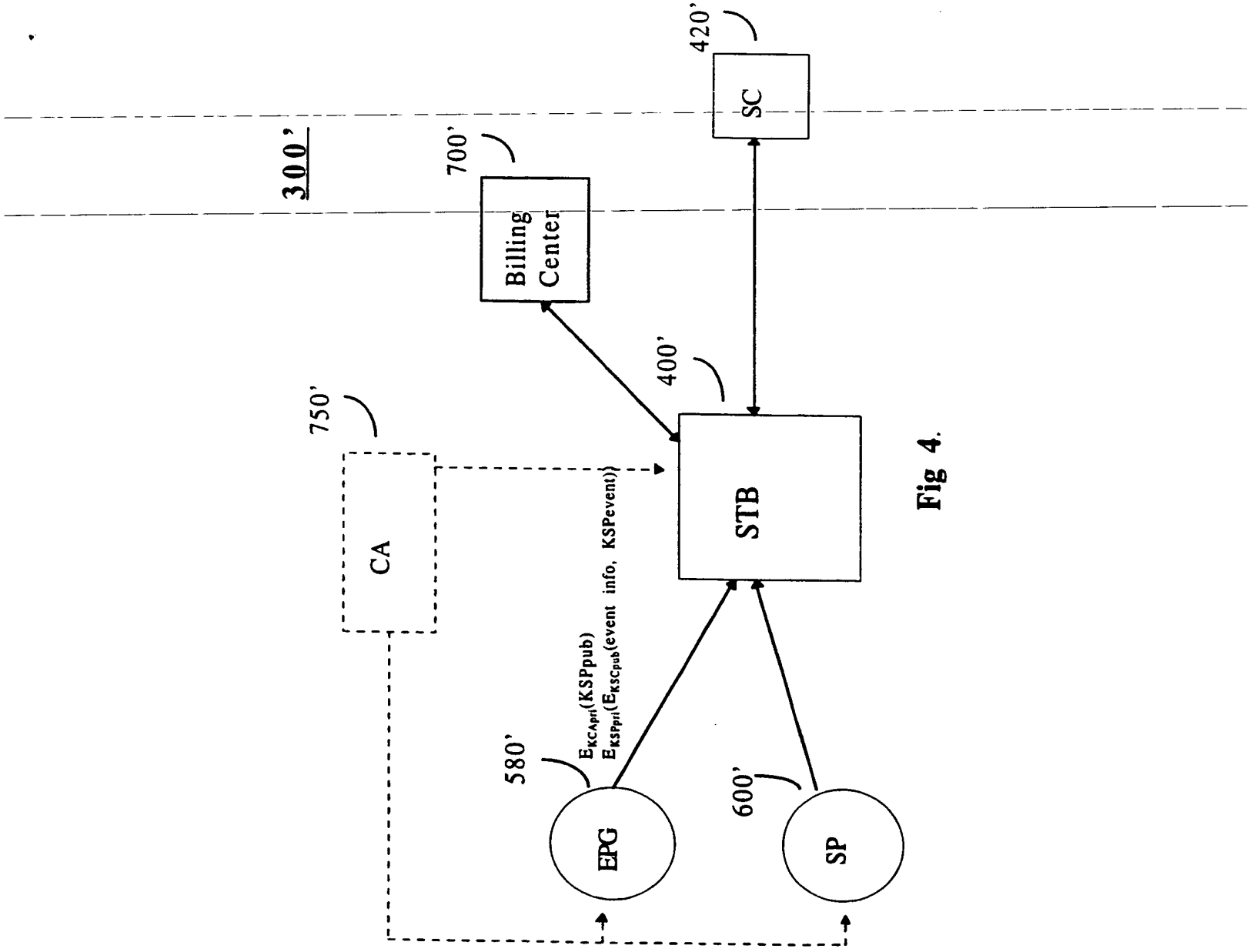

300'
420'
SC
700'
Billing Center
400'
750'
CA
STB
580'
$E_{KCApri}(KSPpub)$
$E_{KSPpri}(E_{KSCpub}(event\ info,\ KSPevent))$
600'
EPG
SP

Fig 4.

INTERNATIONAL SEARCH REPORT

Int :tional Application No
PCT/US 98/11634

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N7/167 H04N7/16 H04N5/00

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04N

Documentation searched other than minimumdocumentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 719 045 A (MITSUBISHI CORP) 26 June 1996	1,10-12
Y	see abstract	2,15-17
A	see column 16, line 53 - column 19, line 12	3-9,13, 14,18-20
	see column 26, line 8 - column 26, line 32	
	see figure 4	

Y	EP 0 585 833 A (NOKIA TECHNOLOGY GMBH) 9 March 1994	2,15-17
A	see abstract	1,18-20
	see column 1, line 31 - column 1, line 38	
	see column 3, line 28 - column 3, line 47	
	see figure 1	

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publicationdate of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of theinternational search	Date of mailing of the international search report
4 September 1998	11/09/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Hampson, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/US 98/11634

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category '	Citation of document, with indication.where appropnate, of the relevant passages	Relevant to claim No.
A	EP 0 506 435 A (SCIENTIFIC ATLANTA) 30 September 1992 see abstract see page 8, line 41 - page 14, line 38 see figures 7,8	1-20
A	SCHOONEVELD VAN D: "STANDARDIZATION OF CONDITIONAL ACCESS SYSTEMS FOR DIGITAL PAY TELEVISION" PHILIPS JOURNAL OF RESEARCH, vol. 50, no. 1/02, July 1996, pages 217-225, XP000627672 see page 217, line 1 - page 219, line 20 see figures 1,2	1-20
A	US 5 592 551 A (HAYASHI MICHAEL T ET AL) 7 January 1997 see column 7, line 19 - column 11, line 7 see figure 3	1-20

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int ional Application No
PCT/US 98/11634

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP 0719045 A	26-06-1996	JP	8288940 A	01-11-1996
		US	5740246 A	14-04-1998
EP 0585833 A	09-03-1994	FI	923980 A	05-03-1994
EP 0506435 A	30-09-1992	US	5237610 A	17-08-1993
		AT	144670 T	15-11-1996
		AU	650958 B	07-07-1994
		AU	1384092 A	01-10-1992
		CN	1066950 A,B	09-12-1992
		DE	69214698 D	28-11-1996
		DE	69214698 T	06-03-1997
		EP	0679029 A	25-10-1995
		EP	0683614 A	22-11-1995
		JP	5145923 A	11-06-1993
		SG	44801 A	19-12-1997
US 5592551 A	07-01-1997	US	5367571 A	22-11-1994
		US	5357276 A	18-10-1994
		AU	684936 B	08-01-1998
		AU	2281495 A	10-11-1995
		BR	9507404 A	07-10-1997
		CA	2187880 A	26-10-1995
		EP	0756797 A	05-02-1997
		FI	964191 A	18-12-1996
		JP	10502501 T	03-03-1998
		NO	964388 A	18-12-1996
		WO	9528799 A	26-10-1995
		US	5537292 A	16-07-1996

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

TRIPOLI, J.
GE & RCA Licensing Management
Operation, Inc.
P.O. Box 5312
Princeton, New Jersey 08543
ETATS-UNIS D'AMERIQUE

JUN 28 1999

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL PRELIMINARY
EXAMINATION REPORT
(PCT Rule 71.1)

Date of mailing *(day/month/year)*	17.06.99
Applicant's or agent's file reference RCA 88674	**IMPORTANT NOTIFICATION**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US98/11634	05/06/1998	06/06/1997

Applicant
THOMSON CONSUMER ELECTRONICS, INC. et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/	Authorized officer
European Patent Office D-80298 Munich Tel. (+49-89) 2399-0 Tx: 523656 epmu d Fax: (+49-89) 2399-4465	Mader, D Tel.(+49-89) 2399-2887

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
RCA 88674		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US98/11634	05/06/1998	06/06/1997
International Patent Classification (IPC) or national classification and IPC H04N7/167		
Applicant THOMSON CONSUMER ELECTRONICS, INC. et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 5 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
21/12/1998	17.06.99
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. (+49-89) 2399-0 Tx: 523656 epmu d Fax: (+49-89) 2399-4465	Authorized officer Glendinning, D Telephone No. (+49-89) 2399 2443

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/US98/11634

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1.3-12.14	as originally filed			
2.13	as received on	07/06/1999	with letter of	04/06/1999

Claims, No.:

1-9	as originally filed			
10-20	as received on	07/06/1999	with letter of	04/06/1999

Drawings, sheets:

1/4-4/4	as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-20
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-20
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

V Reasoned statement under Article 35(2)

1 The present invention relates to a method whereby a user can select an event from an electronic list of events, such as a program guide for television. Associated with each event in the list is a message and a digital signature, the latter to be used for authenticating the provider of that event. The message includes an event key which has been used to scramble the event in question. The digital signature was created using a 1st private key and the user who wishes to select that event authenticates the signature using a 1st public key. The message was encrypted using a 2nd public key and the user decrypts the message using a 2nd private key - the user thereby obtains the event key which is then used to descramble the selected event.

2 Electronic lists of events, such as TV program guides, are widely known and there is extensive disclosure of public key encryption systems in EP-A-0 719 045. However, whilst the EP document does disclose the use of digital signatures encrypted using a public key system, and whilst it does disclose the transmission in encrypted form of keys used to encrypt the event in question, none of the many alternatives put forward in the EP document clearly corresponds to or suggests the method set out above in paragraph 1, and so the claimed subject matter is considered to be new and to have inventive step.

provider. Connections to the internet or world-wide web (web) are usually handled via a personal computer 14, or the like, and a modem 20. Traditionally, access to the internet is managed using a specially designed software package loaded onto the computer; this software enables a user to connect to an internet service provider who acts as the gate keeper to the web. The user typically pays a monthly fee to the service provider for access to the internet, either on a limited or unlimited basis. As one would expect there are numerous service providers, each which requires specialized software for access.

United States Patent Application Number US 5,592,551 teaches the transmission of lists of events (or program guides). European Patent Application Number EP-A-0 719 045 teaches a crypt key system in which the user provides the key necessary for decrypting to the broadcasting station. Particularly, the broadcasting station 11 broadcasts a public-key Kbd or a public-key pair using the scanning lines during the retrace blanking interval period of an analog television picture (col. 8, lines 50-58). The user sends a message comprising its secret key Ksu encrypted by the received public-key Kbd (col. 9, lines 14-25). The user's secret key Ksu is obtained using the corresponding private-key Kvd (col. 9, lines 26-30). The requested program is encrypted using the user's secret key Ksu, and then transmitted to the user via communication apparatus 15 and communication line 17 where it is decrypted using Ksu (col. 9, lines 31-44).

Summary of the Invention

The manufacturers of these digital televisions and set-top boxes may desire that they be compensated by the service provider for each connection to the service emanating from the box. Thus, the flexibility of open hardware architecture of the televisions and the set-top boxes in combination with a competitive market for such devices necessitates the need to provide a system for managing access so that the manufacturer is compensated for any use of its hardware to access any selected service provider. This invention resides, in part, in recognition of the described problem and, in part, in providing a solution to the problem.

An event or program as described herein comprises one of the following: (1) audio/visual data such as a movie, weekly "television" show or a documentary; (2) textual data such as an electronic magazine, paper, or weather news; (3) computer software; (4) binary data such as images or (5) HTML data (e.g., web pages). These service providers include any provider broadcasting events, for example,

message. This encrypted message would only contain information related to the event, that is, the event key would not be included. In such an embodiment, public key cryptography may be used to encrypt the broadcast event. The electronic program guide must still be authenticated in STB 400 as described above. However, the decrypted message only contains information corresponding to the selected event. This information is stored and must be used by SC 420 to determine the private key for decrypting the event. In this embodiment utilizing public key cryptography, key transport is not needed.

The present invention has been described in terms of exemplary embodiments in which a single smart card cooperates with a single set-top box to manage access to a single service provider. However, it is within the scope of this invention to provide a conditional access system which may be extended to permit the smart card to "roam" across (i.e., provide conditional access between) multiple service providers and multiple manufacturers of the set-top boxes.

The robustness of the defined system may be increased by encrypting portions of the event with different keys included in the broadcast stream. Each of these different keys (which are used to decrypt a portion of the event) may be protected using the symmetric key received from the electronic program source.

While the invention has been described in detail with respect to numerous embodiments thereof, it will be apparent that upon reading and understanding of the foregoing, numerous alterations to the described embodiment will occur to those skilled in

10. The method of Claim 1 wherein said digital signature, said first public key and said first private key are issued by an independent certificate authority and are associated with said list provider.

11. The method of Claim 10 wherein said device is a digital television.

12. The method of Claim 10 wherein said device is a set-top box.

13. The method of Claim 4 wherein said event information is used within said device to update said user's account information.

14. The method of Claim 13 wherein said event information is downloaded to an independent billing center to update a user's account information.

15. A method for managing access between a device having a smart card coupled thereto and a service provider, said device performing the steps of:

(a) receiving an electronic program guide from a guide provider, said guide having a digitally signed message corresponding to each event in said guide, each of said digitally signed messages comprise a message encrypted using a public key of the smart card and a digital signature created using a private key of said guide provider;

(b) selecting an event from said guide;

(c) receiving said digitally signed message corresponding to the selected event;

(d) authenticating said guide provider by decrypting said digital signature using a public key of said guide provider, said guide public key being stored in said device;

(e) passing said message to a smart card coupled to the device;

(f) decrypting said message using a private key of the smart card to obtain event information and a symmetric key, said smart card private key being stored within the smart card;

(g) storing said event information in the smart card and updating account information based on said event information;

(h) receiving from the service provider said selected event, said selected event being scrambled using said symmetric key; and

(i) descrambling, in said smart card, said selected event using said symmetric key to generate a descrambled event.

16. The method of Claim 15 wherein the device is a set-top box.

17. The method of Claim 15 wherein the device is a digital television.

18. A method for managing access between a device having a smart card coupled thereto and a service provider, said device performing the steps of:

(a) receiving an electronic program guide, said guide having a digital certificate and a separate message corresponding to each event in said guide, each of said digital certificates being encrypted using a first private key of said guide, said separate message being encrypted using a public key of the smart card and having an associated digital signature created using a second private key of said guide;

(b) selecting an event from said guide;

(c) receiving said digital certificate, said message and said digital signature corresponding to the selected event;

(d) authenticating said guide provider by decrypting said digital certificate using a first public key of said guide to obtain a second public key of said guide, and decrypting said digital signature using said second guide public key, said first guide public key being stored in the device;

(e) passing said message to said smart card;

(f) decrypting said message using a s private key of the smart card to obtain event information and a symmetric key, said smart card private key being stored within the smart card;

(g) storing said event information in the smart card and updating account information based on said event information;

(h) receiving from the service provider said selected event, said selected event being scrambled using said symmetric key; and

(i) descrambling, in said smart card, said selected event using said symmetric key to generate a descrambled event.

19. The method of Claim 18 wherein the device is a set-top box.

20. The method of Claim 18 wherein the device is a digital television.